AFFIDAVIT

I, Charles E. Shevlin, state:

1. I have been a Special Agent with Internal Revenue Service Criminal Investigation, United States Department of Treasury ("IRS-CI") since July 2017. My duties include the investigation of criminal violations of the Internal Revenue Code and related statutes. From July 2017 through February 2018, I attended the Federal Law Enforcement Training Center in Glynco, Georgia, where I received training in conducting financial investigations and in IRS-CI policies and procedures. I also received training in the use of law enforcement techniques such as search and seizure warrants.

2. From September 2014 through May 2017, I was employed as a Staff Accountant. As a Staff Accountant, I kept the books for companies, prepared financial statements, and prepared federal and state corporate, partnership and individual income tax returns. I hold a Bachelor of Arts degree in Accounting from Siena College and a Masters in Accounting from the University of Massachusetts, Lowell.

3. As a Special Agent, I have participated in the execution of numerous search warrants related to several criminal investigations. Through training and prior work experience, I have become familiar with the types of records businesses typically maintain in the course of their regular activity, including ledgers, journals, invoices, receipts, bank documents, and client files.

4. I am currently investigating Ronald McPhail ("McPhail"), acting individually and through his companies Ronald McPhail Roofing LLC ("RMR") and Ronald McPhail Siding and Roofing LLC ("RMSRLLC"), for attempting to evade or defeat the assessment or payment of tax in violation of 26 U.S.C. §7201, filing false tax returns in violation of 26 U.S.C. §7206(1), and

structuring financial transactions to avoid a reporting requirement in violation of 31 U.S.C. §5324, for the tax years 2014 through 2019 ("the Target Offenses").

5. I submit this affidavit in support of an application for a warrant under Fed. R. Crim. P. 41 to search McPhail's residence and the business premises of RMSRLLC and RMR, all of which are located at [redacted] Windham, New Hampshire [redacted] ("the Subject Premises"). The Subject Premises is described more fully in Attachment A to the proposed warrant for the Subject Premises.

6. There is probable cause to believe for the reasons stated below that the Subject Premises will contain evidence, fruits, and instrumentalities of the Target Offenses, all as described in Attachment B to the proposed warrant to search the Subject Premises.

7. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested search warrant and does not set forth all my knowledge about this matter.

BACKGROUND

8. McPhail has owned and operated RMR since 2005. RMR, which was established in New Hampshire that year as a limited liability company, is a roofing company located at the Subject Premises.

9. For at least the tax years 2014 through 2017, the income and expenses of RMR were reported on McPhail's Form 1040, U.S. Individual Income Tax Return, Schedule C.

10. In 2017, RMR was re-organized in New Hampshire as RMSRLLC, a limited liability company also located at the Subject Premises. RMSRLLC's income and expenses were reported on a Form 1065, U.S. Return of Partnership Income for the tax years 2017 through

2019.

11. As a partnership, RMSRLLC's profits and losses were passed directly to its partners. For 2017, these profits and losses were split among: McPhail (64%); Kenneth Roy (18%); and Daniel Robinson (18%). For 2018, the profits and losses were split among: McPhail (49%); Robinson (19%); Jeremy Gravlin (19%); and Jarret Kazanjian (13%). For 2019, the profits and losses were split among: McPhail (36%); Robinson (16%), Gravlin (16%), Garrett McPhail (16%), and Boyd Foulds (16%). In all three years, the partners were then taxed at their respective individual income tax rates for their shares of RMSRLLC's income and expenses when they filed their individual tax returns.

THE SUBJECT PREMISES WILL CONTAIN EVIDENCE, FRUITS AND INSTRUMENTALITIES OF THE TARGET OFFENSES

12. A review of public records reveals that McPhail currently owns the Subject Premises.

13. Records from the Massachusetts Secretary of the Commonwealth indicate that McPhail incorporated RMR and that the principal office for the company is located at the Subject Premises.

14. Records from the New Hampshire Secretary of State show that RMR was incorporated and operated with a principal office address of the Subject Premises.

15. Records from the New Hampshire Secretary of State also show that RMSRLLC was incorporated and registered with a principal office and mailing address of the Subject Premises.

16. The business address listed on RMSRLLC's partnership tax return (Form 1065) for 2017 through 2019 is the Subject Premises. The business address listed for RMR on the

Schedule C of McPhail's individual income tax return (Form 1040) for the years 2013 through 2017 is the Subject Premises.

17. McPhail's individual income tax returns for the years 2014 through 2017 also indicate that he uses the Subject Premises to conduct RMS and RMSRLLC's business. Specifically, McPhail has claimed that 170 square feet of his home (*i.e.*, the Subject Premises) is used exclusively for business purposes.

18. A mail cover was conducted on the address of the Subject Premises between April 8, 2019 and May 7, 2019. Mail for both RMR and RMRSLLC was received during this time frame at the Subject Premises, including from Hi-Ho Container Service & Metals Recycling, Harvey Building Products, Jeanne D'Arc Credit Union, and Mark and Kristine Finocchario.

19. Bank records obtained from Jeanne D'Arc Credit Union show that RMSRLLC maintains a business checking account at that credit union; and that payments from RMSRLLC's business checking account were made to both Hi-Ho Container Service & Metals Recycling and Harvey Building Products. This indicates to me based on my training and experience that RMSRLLC contractors or suppliers send mail to RMSRLLC at the Subject Premises.

20. Bank records similarly show that checks from Mark and Kristine Finocchario were deposited into the RMSRLLC business bank account in March and April of 2019 with memo lines indicating: "new roof," "my ½ of Haverhill house," and "roof repair." This indicates to me based on my training and experience that McPhail's customers send payment to him for RMSRLLC's work at the Subject Premises.

21. Through my training and experience, I know that it is typical for businesses to keep detailed records of their customers' accounts, accounts receivable, payments received, payroll and other financial details at their business locations. These record are typically used to

monitor the financial state of the business, track income and expenses, and aid in the preparation of federal and state income tax returns.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

22. Based on information received during the course of this investigation, there is probable cause to believe that McPhail has substantially underreported RMR and RMSRLLC's gross receipts on his Form 1040, Schedule C for the tax years 2014 through 2017, and on RMSRLLC's Form 1065 for the tax years 2017 through 2019. There is also probable cause to believe that he thereby under-reported his total income on his Form 1040 for 2014 through 2019, resulting in a substantial tax due and owing on that unreported income.

23. As detailed below, the primary source of information for this affidavit is financial records obtained from banks where McPhail, RMR, and RMSRLLC maintained accounts.

Underreporting Of Income

24. For the years 2013 through 2019, records obtained from Jeanne D'Arc Credit Union and TD Bank indicate that RMR and RMSRLLC received deposits into their respective business checking accounts as set forth in the table below:

Year	2013	2014	2015	2016	2017	2018	2019
Business Checking Deposits	$402,539	$621,648,	$733,009	$568,405	$924,355	$1,417,093	$1,373,723

25. Records obtained from Jeanne D'Arc Credit Union and TD Bank indicate that between 2014 and 2019, McPhail cashed against his personal bank account and the bank accounts of RMR and RMSRLLC (but did not deposit) at least 744 checks in the amounts described in the table below at various Jeanne D'Arc branches.

26. Many of these checks, where provided by the financial institutions, show memo notations such as "roof," "siding," and other content that causes me to believe they are in payment by customers for McPhail's services, and would ordinarily constitute business receipts that should be reported on income tax returns.

27. Many of these checks that McPhail cashed were structured, meaning that they were cashed in groups whose amounts totaled just under $10,000.00. Frequently, McPhail received multiple checks from the same individuals, dated the same day and in sequential order, that were ultimately cashed on different dates and, in many cases, at different branches of Jeanne D'Arc Credit Union.

McPhail Checks Cashed But Not Deposited at Jeanne D'Arc CU	
Year	**Checks Cashed**
2014	$343,509
2015	$420,213
2016	$295,339
2017	$758,015
2018	$980,013
2019	$1,067,646

28. Based on my training and experience investigating criminal tax matters, I am aware that one way in which businesses evade the payment of income taxes is to reduce the amount of gross receipts that appear in the business' bank account. When expenses are deducted from a lowered amount of gross receipts, the tax due and owing on the business' reported income is lower.

29. McPhail's behavior also indicates to me an effort to avoid reporting his cashing of more than $10,000 in checks at a time to the Internal Revenue Service on a FinCEN CTR, which may violate Title 31, United States Code, Section 5324.

30. From 2014 through 2019, notwithstanding the cashing of the checks described above, RMR and RMSRLLC reported the following business gross receipts and net income on the companies' respective Forms 1040 (for RMR) and Forms 1065 (for RMSRLLC):

Year	Gross Receipts	Net Income
2014	468,223	93,442
2015	559,526	75,005
2016	401,459	84,124
2017	918,529	90,121
2018	1,291,196	-5,916
2019	1,325,580	-13,148

31. For the tax years 2017 through 2019, the revenues, income, and expenses present on McPhail, RMR and RMSRLLC's federal income tax returns all appear to be generated from the business bank account records of RMR and RMSRLLC. Business checks that were cashed and not deposited are not present in the business bank account's statements and thus appear not to have been included in McPhail, RMR, and RMSRLLC's federal income tax returns. As noted above, based on my training and experience investigating criminal tax matters, I know that cashing business related checks is a method used to keep business income out of the business bank accounts and thus off any income tax returns generated from the business bank account records, all in aid of underreporting income.

32. For the period 2014 through 2016, however, gross receipts reported on RMR and McPhail's income tax returns were less than what was deposited into RMR's business bank account, which indicates to me that not only did RMR and McPhail's returns underreport gross receipts by the amount of the cashed checks, but also that the returns underreported other, deposited business receipts.

33. Comparing the total amount of gross receipts deposited and checks cashed—which I believe based on my training and experience is the actual amount of gross receipts—and what is reported on RMR, RMSRLLC and McPhail's tax returns shows significant discrepancies between the bank records and what is reported on the returns. Specifically, McPhail, RMR, and RMRSLLC appear to have underreported approximately $4.5 million in gross receipts.

Year	Deposits into Business Bank Accounts	Checks Cashed	Gross Receipts		Suspected Unreported Gross Receipts
			Per Bank Records	Per Tax Returns	
2014	621,648	343,509	965,157	468,223	496,934
2015	733,009	420,213	1,153,222	559,526	593,696
2016	568,405	295,339	863,744	401,459	462,285
2017	924,355	758,015	1,682,370	918,529	763,841
2018	1,417,093	980,013	2,397,106	1,291,196	1,105,910
2019	1,373,723	1,067,646	2,440,880	1,325,380	1,115,500

34. As noted above, this causes me to believe that McPhail is substantially under-reporting his gross receipts (and thereby his income) by omitting receipts contained within checks he cashes.[1]

35. According to the returns filed with the IRS, McPhail uses paid tax return preparers to prepare both his personal Form 1040s and RMSRLLC's Form 1065s tax returns. McPhail's personal returns were prepared by Emily Haswell, CPA, of the Olbricht Storniolo

[1] While it is possible that McPhail uses the checks he cashes to pay for business expenses, these expenses do not appear to be reported on the business' or McPhail's returns. In either case, however, there is probable cause to believe that the business' records regarding its receipts and expenses will be found within the Subject Premises. Similarly, even if McPhail uses the checks he cashes to fund a cash payroll, records of that activity would likely evidence an attempt to avoid the payment of payroll taxes in violation of one of the Target Offenses.

Group, for 2013 through 2016, and by Joel Olbricht in 2017 and 2018. McPhail's 2019 personal return was not prepared by a paid return preparer. RMSRLLC's Forms 1065 for 2017 through 2019 were prepared by Joel C. Olbricht.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

36. From my training, experience, and information provided to me by other agents, I am aware that businesses frequently use computers to carry out, communicate about, and store records about their business operations. These tasks are frequently accomplished through sending and receiving business-related email and instant messages; drafting other business documents such as spreadsheets and presentations; scheduling business activities; keeping a calendar of business and other activities; arranging for business travel; storing pictures related to business activities; purchasing and selling inventory and supplies online; researching online; and accessing banking, financial, investment, utility, and other accounts concerning the movement and payment of money online.

37. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

38. Additionally, RMSRLLC maintains a business website, Facebook page, and an e-mail account associated with the business. From my training, experience, and information

provided to me by other agents, I am aware that websites, Facebook pages, and e-mail accounts are typically accessed, updated, and maintained through the use of computers or cell phones. RMRSLCC's website and Facebook page feature photos of the company's work, contact information, reviews, and vendor information. Records of photos uploaded to websites or Facebook page are typically stored on computers and cell phones. Such records could provide information about clients and can be used to identify unreported income.

39. From my training, experience, and information provided to me by other agents, I am aware that businesses and individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones and storage media. Furthermore, smartphones can be operated as mobile recording keeping devices and can be used to keep detailed calendars, work schedules, take photos of work performed, used to send communications with clients and employees through text messages. These records would be instrumental in identifying unreported income or employees paid in cash.

40. Based on my knowledge, training, experience and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore when users replace their computers, they can easily transfer the data from their old computer to their new computer.

41. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

42. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

43. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

44. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

45. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may

provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

46. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them and when.

47. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a

computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

48. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. In addition, based on my knowledge, training, and experience, I know that businesses and businesspeople often retain correspondence, financial, transactional, and other business records for years to identify past customers and vendors for potential future transactions; keep track of business deals; monitor payments, debts, and expenses; resolve business disputes stemming from past transactions; prepare tax returns and other tax documents; and engage in other business-related purposes.

50. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where is it seized. This is true because of:

51. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or

with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

52. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

53. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

54. The Subject Premises may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer

equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

55. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) MCPHAIL, RMR, and/or RMSRLLC. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

56. In this case, I recognize that RMSRLLC is a functioning company that performs some legitimate business functions, and that seizing computer equipment may have the unintended and undesired effect of limiting the company's ability to function.

57. As stated above, there are a variety of reasons why law enforcement agents might need to seize the computer equipment for subsequent processing elsewhere. If McPhail requires access to data that is not contraband or evidence of a crime, the government will work with the company after the search to copy this data onto storage media provided by the company for the company's use.

58. If the search team determines that there is no reason to seize certain RMR or RMSRLLC computer equipment during the execution of this warrant, the team will create an onsite electronic "image" of those parts that are likely to store data specified in the warrant, if imaging is practical. Generally speaking, imaging is the taking of a complete electronic picture of the data, including all hidden sectors and deleted files. Imaging permits the agents to obtain an

exact copy of the computer's stored data without actually seizing the computer equipment. However, imaging at the premises can often be impractical, because imaging is resource-intensive: it can take hours or days, thus requiring law enforcement agents to remain at the premises for much longer than they would remain if they seized the items, and it can require personnel with specialized experience and specialized equipment, both of which might be unavailable. If law enforcement personnel do create an image at the premises, they will then search for the records and data specified in the warrant from the image copy at a later date off-site.

59. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the IRS may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

60. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

61. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

62. The passcode that would unlock the device(s) found during the search of the Subject Premises is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of the device(s) found during the search of the Subject Premises to the device's fingerprint sensor or to hold the device up to the face of the owner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

63. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of McPhail at the Subject Premises to the sensor of the devices or place the devices in front of his face for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

64. Based on the information described above, there is probable cause to believe that McPhail has violated the Target Offenses.

65. Based on the information described above, there is also probable cause to believe that evidence, fruits and instrumentalities of these crimes, as described in Attachment B to the warrant, are contained within the premises described in Attachment A to the warrant to search the premises.

/s/ Charles Shevlin
Charles Shevlin
Special Agent
Internal Revenue Service, Criminal Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Oct 30, 2020 /s/ Andrea K. Johnstone
Hon. Andrea K. Johnstone
Time: 3:08 PM, Oct 30, 2020 U.S. Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched are located at 34 Nottingham Road in Windham, New Hampshire 03087 (the "Subject Premises"). The Subject Premises is a multi-story residential building with a brick façade, green shutters and neutral siding on the sides of the building. The building contains a large window over the front door. There is a small stone pillar at the foot of the driveway with the number "34" affixed to it. The following are photographs of the Subject Premises as seen from Nottingham Road:

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records for the years 2014 to the present in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 26 U.S.C. §7201, 26 U.S.C. §7206(1), and 31 U.S.C. §5324, including:

a. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by

i. Records and tangible objects pertaining to the payment, receipts, transfer, or storage of money or other things of value by Ronald McPhail Roofing LLC, Ronald McPhail Siding and Roofing LLC, Ronald McPhail, Sonata McPhail, Kenneth Roy, Daniel Robinson, Jeremy Gravlin, Jarret Kazanjian, Garrett McPhail, and Boyd Foulds, including:

1. Bank, credit union, investment, money transfer, and other financial account records;
2. Credit and debit card account records;
3. Copies of all federal and state tax returns and work papers;
4. Records pertaining to business or personal expenses;
5. Records pertaining to income, whether from wages or investments;
6. All loan and mortgage agreements and transactions, and lease and rental agreements and transactions, including repayment schedules of principal and interest;

7. General ledgers, general journals, sales journals, cash receipts journals, purchases journals, cash disbursement journals, and any other records that record income and expenses;
8. Invoices, inventory sheets, daily reconciliations, receipts for cash payments, cash register tapes, depreciation schedules and work papers, trial balances, financial statements, credit card receipts, and adjusting entries;
9. Receipts, requests for payments, cancelled checks, and other documents and records evidencing payments requested or received for goods;
10. Personnel and pay records for current and former employees, including records reflecting employee name, job title, social security number, or other designation, salary schedules, as well as all federal tax forms, including but not limited to W-2 and 1099 forms, 941 quarterly tax returns, 940 tax returns;
11. Financial documents and ledgers showing deposits, payments and withdrawals, bank checks, wire transactions, money orders, bank statements, and similar documents reflecting receipts and disbursements of funds;
12. Documents and records pertaining to cash transactions, including receipts from cash deposits, disbursements or withdrawals, or cash or cash equivalents;

13. All register tapes, Z-tapes, QuickBooks Reports or any other print out which would reflect sales activities;
14. Records pertaining to gambling, including gambling losses and gains, and travel to and from gambling locations.

ii. Contracts, agreements, and other documentation evidencing affiliation or business relationships with distributors, suppliers, and records verifying or concerning financial dealings with such distributors and suppliers;

iii. Documents that would be utilized to prepare Federal and State Income Tax Returns;

iv. All currency and other monetary instruments;

v. QuickBooks or comparable accounting software.

vi. Any and all documents and communications with tax preparer Emily Haswell, Joel Olbricht, or the accounting firm Olbricht Storniolio Group LLC

vii. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. Evidence of who used, owned, or controlled the computer equipment;
2. Evidence of computer software that would allow others to control items, evidence of the lack of such malicious software,

and evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the attachment of other computer hardware or storage media;
4. Evidence of counter-forensic programs and associated data that are designed to eliminate data;
5. Evidence of the times that computer equipment was use;
6. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
7. Records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data storage media; and

viii. Records and tangible objects relating to ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

DEFINITIONS

For the purpose of this warrant:

i. “Computer equipment” means any computer hardware, computer software, computer-related documentation, storage media, and data.

ii. “Computer hardware” means any electronic device capable of data processing (such as a computer, personal digital assistant, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

iii. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

iv. “Computer-related documentation” means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

v. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

vi. “Data” means all information stored on storage media of any form in any storage format and for any purpose.

vii. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If, after inspecting seized computer equipment, the government determines that the equipment does not contain contraband or the passwords, account information, or personally identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned, within a reasonable time, if the party seeking return will stipulate for a forensic copy's authenticity (but not necessary relevancy or admissibility) for evidentiary purpose.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; password, account information, or personally identifying information of victims; or the fruits or instrumentalities of crime.